21 CFR Part 11
第6部　バイオメトリック認証：その限界と可能性

テクニカルノート

Wolfgang Winter, Ludwig Huber, Agilent Technologies

あなたの実験室の装置はあなた自身を認識するだろうか？ ラボのバイオメトリックセキュリティシステムは、あなたの指紋や網膜を読んだり、あなたの手相や掌紋をチェックしたり、またはあなたの声や署名を認識することができる。これらのツールを用いて、あなたの業務をより効率的に、かつあなたのデータをより安全にするかどうかを決定することができるのは、あなた自身とあなたのラボだけである。あるいは、あなたが使用する化学物質やあなたがラボで着けている手袋とマスクがこのようなツールを無効にするのだろうか？

本シリーズの1-5部では，データセキュリティ、データインテグリティ、長期保管および迅速なデータ復元に焦点を合わせて、電子署名と電子記録に関するFDA規則（21CFR Part 11）の要求事項を要約した（1−5)。我々は、システムと重要な機能に対するどのようなアクセスが、権限を与えられた者に制限され得るかを示した。データの解析と評価の時点でどんなデータインテグリティが保証されるか、また、記録の作成、変更および削除がコンピュータの生成する監査証跡にどのように記入されるかも示した。我々はデータをアーカイブして、数年後にそれを正確に取り出すための最良の方法を示した。さらに、我々は機器コントロールの技術的側面を見た。そのすべてが、アクセスとデータセキュリティを保証するため、自然とバイオメトリック認証メカニズムの議論に結び付く。

「従来の」認証スキーム

21CFR Part 11の要求事項は、電子記録の信頼性を保証するために技術制御手段に権限を与える。この制御手段にはアクセスセキュリティのためのメカニズムと権限チェックが含まれる。我々は以前、Windows NT（Microsoft, Redmond, WA）などの近代的なオペレーティングシステムで利用可能な認証スキームを実行するために、ユーザアカウントとパスワードポリシーを管理する重要性について議論した（2)。Trust in Cyberspace［サイバースペースを信用する］で、Schneiderは「認証は、指定された（あるいは暗黙の）信頼レベルで断言される身元（アイデンティティ）を確認する工程である」と書いている（6)。そのようなシステムにおける従来の（かつ最も多用されている）認証スキームは、通常、パスワードや暗証番号（PIN）などのユーザが知っていること、あるいはトークン、IDカード、ICカードなどのユーザが所持しているもののいずれかを基にしている（7)。

Part 11の要求事項によると、このような認証スキームは、手続き上もしくは行動に関する手順によって補足する必要があり、この手順でパスワードやトークンのプライバシーと機密保持を保証して他人に成り済ますことを防止する。例えば、成り済ましには少なくとも2個人の協力を必要とするように、制御手段は設計されなければならない（8)。

身元確認するバイオメトリクス（生物測定学）

従来の認証メカニズムと異なり、バイオメトリクス（生物測定学）では、ユーザが実在すること（9)、あるいは指紋などの個々人に固有のもの（6）を基にする。Woodwardが説明したように、バイオメトリクスは「非常に古くて簡単なコンセプト：人間の認識」に基づくものなので、バイオメトリクスの考えは新しいものでもハイテクでもない（9)。バイオメトリクスはある個人の物理的あるいは行動上の特徴を自動的に測定し、あらかじめ測定しておいた記録との比較によって、その個人のアイデンティティ（同一性）を確認するものである。バイオメトリクスの例には、指紋分析、スピーチパターン認識、手や顔の幾何学的な形および虹

彩や網膜のスキャンがある（表1）。

要求事項ではない Part 11が開発された時点においては、バイオメトリック認証メカニズムは一般に利用できなかっただけでなく、コンピュータのハードウェアとソフトウェアのシステムも確実にサポートしていなかった。規則の意図は、規制が実施された後で開発される新しい技術の使用を見越して可能にすることにある。以前に議論したように、FDAによる規制を受ける産業におけるほとんどの環境ではクローズドシステムが考慮されている ― また、クローズドシステムは暗号化技術やバイオメトリクスを必要としない（1）。

オープンシステム（会社は電子記録の内容に責任を持つものの、このシステム自体へのアクセスを管理しないシステムなど）は、アクセスセキュリティのためのデジタル署名やデータインテグリティと機密保持のための暗号化などの高度な技術なくして、Part 11を遵守することができない。

従来の認証におけるリスクへの対応 従来の認証スキームを使用する場合のリスクは、現金自動預払機（ATM）取引における銀行カードの例が広く知られている。「従来の認証のリスク」ボックスには、このようなタイプの危険性が記載されている。

一般的に、異なったシステムのために別個のパスワードを選び、さらに適切なパスワードポリシーを実施することによって、これらのリスクが管理される。たとえ従来のスキームに問題が生じたとしても、システムへの今後のアクセスにおいて問題の原因を修正することができる。このことは金属製の鍵によるセキュリティに類似している。鍵は更新（変更）することができ、また破壊することもできる。鍵に問題が生じれば、あなたは錠前を交換（鍵を更新）することができ、あなたの所有物は再び安全になる。

バイオメトリックアプリケーション 我々の多くは既に我々の日課の中でバイオメトリクスに触れている。合衆国に頻繁に出入りする旅行者は、ニューアークやサンフランシスコなどの空港

表1. バイオメトリクスの主な種類。R. D. McDowall, "Biometrics: The Password You'll Never Forget（バイオメトリクス：あなたが決して忘れないパスワード）," LCGC Eur. 13（10）, p.736 （2000） から引用

バイオメトリック媒体	主な特徴
顔の形の認証 (Face recognition)	原理：顔の特徴の独特の形、パターン、および配置の分析。非常に複雑な技術で、主としてソフトウェアベース。 本質的に2つの読み取り方法：ビデオあるいは赤外線画像を利用。後者は赤外線カメラが高コストなので、より高価。 主な利点は、バイオメトリックシステムは「ハンズフリー」で操作できること、単にスクリーンを見つめるだけでユーザのアイデンティティが確認されること。 ユーザの連続モニタリング。 ユーザがカメラの視野から外れた場合に、機密情報へのアクセスを無効にできる。 その後、ユーザが作業するためにデスクトップに戻ると、照合が実行される。
指のスキャン (Finger scanning)	原理： 詳細部分の分析（指の画像隆線［検証］終端点、分岐点または隆線の分岐）。 最も商業的に成功しているバイオメトリック技術の1つ。 立ち入る人のアイデンティティを検証するために必要となるアプリケーションにおいて重要。
手の幾何学的な形 (Hand geometry)	原理：ハンドリーダーに載せた手の立体画像をカメラで撮影。 非常に弾力性があり、エンドユーザのスループットを高くできる。
指の幾何学的な形 (Finger geometry)	原理：手の幾何学的な形と同様の原則を用いて、指の立体画像をカメラで撮影。 物理的なアクセス管理領域で立証済み。 非常に耐久性があり、外部的条件をうまく処理。
虹彩認証（Iris recognition）	原理：虹彩（目の瞳孔を取り囲む組織の有色の輪）の分析。 多くのアプリケーション領域で折り紙付の業績を有する、非常に成熟した技術。
手のひら（Palm）	原則：指のスキャンで採用されている技術に類似。手のひらに見られる紋様を利用。
網膜（Retina）	原理：網膜は眼底に位置する血管の層。網膜からデータを得るためのスキャン技法は、エンドユーザの多くが最も迷惑に感じるものと考えられる。エンドユーザは緑色のドットに焦点を合わせる必要があり、この実行時に、システムは無害な光線を使用して固有の網膜の特徴を取得する。 すべてのバイオメトリクスの中で最も正確であると考えられる。
署名（Signature）	原理：署名の静的なイメージよりむしろ署名している間のペンの動き。 署名している間のペン圧、ペンが紙に触れる音、あるいはペンの角度など行動に関するバイオメトリクスとなる多くの場面が研究対象となり得る。 我々は、我々の名前を署名することを学び、この学習プロセスのおかげで我々の署名は独特になる。署名の速さ、速度、および圧力は、ほぼ一定している。 署名システムには専用のタブレットや専用のペンが必要。
音声認識（Voice recognition）	原理：物理的な特性と行動的な特性を融合した声に特有な特性（喉頭の物理的な大きさと身に付いた話し方を採り入れた音響）の分析。 ハードウェアはほとんど不必要（特有の特性を解析するためのソフトウェアを搭載した標準的なPCのマイクロホン）。 理想的には電話ベースのアプリケーションに適す。

従来の認証におけるリスク

パスワードはスパイされたり見られたりして「盗まれる」。

貧弱なパスワードは推測されたり、辞書ベースのセキュリティ攻撃ツールによる攻撃を受けて「解読」されたりする可能性がある。

同じパスワードがもう1つの別のシステムで使用されている場合、パスワードが危うくなるリスクは2倍に増加する。

パスワードは失くしたり忘れたりすることがある。多くのパスワードは、便利だという理由から、コンピュータ周辺のどこかに書き留められていたために危険に曝されてきた。

で、米国入国審査簡易プログラム（INSPASS）による必要なアイデンティティをバリデーションするための手の幾何学的な形スキャナを使用したかもしれない（10）。この仕組みは入国審査を抜本的にスピードアップしている。

健康管理においては、指紋スキャンとICカードによって対象者の探索とカルテの入手を加速している。また、この方法は連絡することができない患者を特定し、医療サービスの誤用を探知する助けにもなる。このようなスキャナの供給者によると、指紋認証システムは「バイオメトリック認証の有力な形式になり、99.9％の正確さであるものの、100万人を超えるデータベースから一個人を確認することも特定することもできない」（11）。もちろん、典型的なラボ環境においては、実際に識別を必要とする人の数は限られており、識別過程がランタイム性能を妨害すべきでもない。

McDowallは、最近、最新のバイオメトリックアプリケーションの概要を発表し（表1）、ラボにおけるアプリケーションにとっての長所と短所それぞれについて議論した（12）。バイオメトリックシステムを選ぶ前に、ラボ環境で通常身につけている防護用具が識別過程をどれほど厄介にするものかを事前評価する必要がある。アプリケーションはフェイスマスクを通して網膜パターンを読むことができるのだろうか？手袋は指紋スキャンのために外す必要があるのだろうか？あなたはどんな化学物質を使用するのだろうか、またその化学物質はスキャナにどんな影響を与えるのだろうか？

バイオメトリック認証におけるリスク

バイオメトリクスでは、ユーザの身体がパスワードになる。このことは、パスワード自体を盗んだり改ざんしたりすることが極めて難しいことを意味する。ユーザは貧弱なパスワードを作成できるが、ユーザは貧弱なバイオメトリックを選ぶことはできない（13）。とはいえ、バイオメトリックシステムのセキュリティに対する攻撃は、次のようなセキュリティチェーンの脆弱部に集中しそうである。入力メカニズムのセキュリティ、バイオメトリック指標のデジタル表示、およびバイオメトリック指標の単一項目性（unarity）（7）など。

永遠に失われる 言い換えると、おそらくセキュリティ攻撃は入力デバイスからではなく、それによって生成されるデータから始まるだろう。Millerは次のように書いている。

パーソナルコンピュータが提供するバイオメトリック認証データは、推定されるスキャニングデバイスが生成したかも知れないし、攻撃者が供給したビット列かも知れない。したがって、正当なバイオメトリックデータであるように見えるビット列を発生させることが可能であるという点では、そのようなシステムは無防備である。その上、バイオメトリックスキャンをバリデーションするために必要なテンプレートの所持、さらにそのテンプレートを作成するために用いるアルゴリズムの知識が、そのようなビット列を発生させるために十分な情報を供給する可能性がある（テンプレートが危ういユーザに対して）。すなわち、任意のバイオメトリック認証サーバに格納されたテンプレートデータを公開は、影響を受けたユーザにとってバイオメトリック技法の使用が永遠に不可能となるおそれがある（7）。

上記のことは、バイオメトリクスの持つ最も大きな危険は、個人のバイオメトリックデータやパラメータがいったん盗まれると、一生を通じて影響を受けてしまうことを意味する。このことは盗まれた鍵の例とは大きく異なる。バイオメトリックは更新したり破壊したりすることができない。もし攻撃者があなたの左手の親指の指紋を示すビット列を所有しているとすると、あなたは左手の親指で決して安全にシステムにアクセスできなくなるだけでなく、攻撃者によるそのビットストリームの使用はあなたに帰することになってしまう。多くのコンピュータ科学者が到達した今日の結論は、「バイオメトリクスは、リーダーから検証者までの接続が安全である状況下では有用である」（12）。

バラツキの許容 2番目の脆弱性は、大部分のバイオメトリックスキームの技術的な実施によってもたらされる。バイオメトリック測定では、測定を通して、またはテストされた特性自体によってもたらされる何らかの可変性を示す複雑なパターンを処理する。例えば、手書きの署名は書くたびにわずかに異なっている。あなたの声が異なって聞こえることもある。または、あなたの指紋のデジタル表示はカットされて改変されるかもしれない。このことは、バイオメトリックアプリケーションにおける一致の決定には組み込まれた許容範囲が必要であることを意味する。しかし、バイオメトリック認証スキームは厳格すぎる許容範囲によって無効にされることもある。この脆弱性は慎重なリスクアセスメントとシステムバリデーションによって管理する必要がある。

プライバシー バイオメトリクスに固有の付加的なリスクは人のプライバシーに関係する。「バイオメトリックは、単一要素からなるアイデンティティで

ある。我々はみんな、左手の親指の指紋は1つしか持っていない。あなたは自分の個人的なアイデンティティから自分の仕事のアイデンティティをどのように分離するだろうか？ヨーロッパのプライバシー要求事項（the OECD Cryptographic Guidelines of 1997, Principle 5［1997年のOECD 暗号ガイドライン、原則5］）に適合させるための米国の不十分な活動と相まって、みなさんの個人的な活動（購入習慣、娯楽の好み、政治活動）が仕事の活動に否応なく結び付けられるという深刻なリスクがある」(14, 15)。

バイオメトリクスの代替手段

コンピュータシステムのセキュリティも、ハードウェアトークンや公開鍵証明書などのように、ユーザが持っていたり知っていたりすることを利用することに由来する。公開鍵証明書は2つの暗号化キーを使用する。最初のキーは情報を暗号化するために、次のキーはこれを解読するために使用される。作成者のみが変更できる文書でもすべての人が読めることを保証するために、暗号解読キー［復号化キー］を利用可能とする（発行する）必要があり、これが公開鍵になる。暗号化キー（秘密鍵）は秘密にしておかれる。対象とするアプリケーションによっては他のバリエーションが可能になる（例えば、秘密性を保証するために、文書を受取人の秘密鍵で解読する必要があるかも知れない)。どちらのキーも暗号化したものを解読できないのでバリエーションが可能である。暗号化キーによる管理の弱点は、キーを支給する必要があること、信頼できる権威者（証明当局）によって人々のアイデンティティを確立し、記録する必要があることである。

ラボへの推奨

必要とされる保証を決めること あなたの分析ラボの認証スキームを定義するときには、従来の認証技術は高度のセキュリティ保証を提供しないということを忘れないことである。しかし、ほとんどのクローズドシステム環境では、しっかりしたセキュリティを含む適切な認証手順とパスワードポリシーの使用によって、最も一般的な手段による記録の劣化を効果的に防いでいる。

目的のための適合性を事前評価すること バイオメトリック認証スキームを決定する前に、それが本当に所期のセキュリティ目的に必要であるかどうかを決めることである。バイオメトリック認証には標準外の追加ハードウェアを必要とすることがあり、システムの残り部分と一緒にバリデーションすることが難しくなる可能性がある。バイオメトリックキーの更新や破壊ができないということを忘れないことである。バイオメトリックキーを傷つけたり失くしたりすると、死ぬまで利用できない。

暗号法を考慮すること あなたが開放環境で働いている場合（例えば、あなたのITインフラがサービスプロバイダに外部委託されている場合)、暗号化認証を考慮する必要がある。多くのIT環境では、ユーザ特有のパスワードを生成させるためにICカードが使用されており、制限された時間内（1分間）は有効で検証サーバと同期している。パスワードは、本人のみが知っているはずの個人的な暗合もしくはPIN（暗証番号）を用いて生成される。ハードウェアのトークンと暗証番号は、盗まれたり改ざんされたりするという本質的なリスクを伴っている。しかし、固定ユーザのログオンとパスワードの組み合わせが改ざんされ易いことと比べれば、そのリスクは小さくなるはずである。

潜在的セキュリティリスクを実践的に事前評価すること John Woodwardは Information Security誌で次のように記している。「大きなソフトウェアシステムは…欠陥なしに開発することはできないものの、脆弱性を予期して事前に対処することによって、そのようなシステムの信頼性を向上させることが可能である」(9)。例えば、あなたはバイオメトリックリーダーからバイオメトリックを検証する処理過程までの接続を保証するために特別な注意を払う必要がある。この接続が潜在的なセキュリティ攻撃に対して無防備な部分だと思われるので、あなたはこの部分が会社や部門の外からアクセスできないように手段を講じる必要がある。

専用のセキュリティ監査ガイドラインを開発すること。政府当局が展開しているセキュリティ監査でこれまでに行われた作業を有効に活用することである。例えば、オーストラリアのニューサウスウェールズのIT局は、セキュリティと監査ログの使用を中心とするグッドリスクアセスメントと監査ガイドラインを発行している（16)。

21CFR Part 11の目的と分析ラボのデータを保証することの目的に関する広大で長期的な観点から、我々の適合性タスクをより容易にするように導いてくれる。我々は以下のようなMoskowitzの発言に賛同する。「我々は、強みを活用して弱点を減らすような方法でセキュリティシステムの作成に専念する必要がある。こうすることで、我々は我々が活動を保証する人達のプライバシーを強化することができる。また我々は、このデジタル時代に必要とされるセキュリティにもかかわらず実行するために、彼らの仕事をより容易にすることができる」(15)。

ギャップを縮めること

本シリーズの最後の論文では、規則が発効するよりずっと以前に設計され、インストールされていたレガシーデータシステムについて、21CFR Part 11が要求する技術制御手段を実行することに焦点を当てる。適切なギャップ分析（適合作業に困難が存在する）と適切な修正アクションプランの所見に基づいて、Part 11の要求事項がどのように満たされるかを議論する。

参考文献

(1) L. Huber,“Implementing 21 CFR Part 11 in Analytical Laboratories: Part 1, Overview and Requirements,”BioPharm 12 (11), 28−34 (1999).（日本語版は，Ludwig Huber，近藤　直人，21 CFR Part 11 試験室における電子署名と電子記録；第一部　規制の概要ならびに要求事項，横河アナリティカルシステムズ，2000年6月，資料番号TI 16C0A3-004）

(2) W. Winter and L. Huber,“Implementing 21 CFR Part 11 in Analytical Laboratories: Part 2, Security Aspects for Systems and Applications,”BioPharm 13 (1), 44-50 (2000).（日本語版は，W. Winter, L. Huber，近藤　直人，21 CFR Part 11 試験室における電子署名と電子記録；第二部　システムとソフトウエアのセキュリティー，横河アナリティカルシステムズ，2000年11月，資料番号TI 16C0A3-005）

(3) W. Winter and L Huber,“Implementing 21 CFR Part 11 in Analytical Laboratories: Part 3, Ensuring Data Integrity in Electronic Records,”BioPharm 13 (3), 45-49 (2000).（日本語版は，W. Winter, L. Huber，近藤　直人，21 CFR Part 11 試験室における電子署名と電子記録；第三部　電子記録の完全性保証，横河アナリティカルシステムズ，2001年4月，資料番号TI 16C0A3-006）

(4) L. Huber and W. Winter,“Implementing 21 CFR Part 11 in Analytical Laboratories: Part 4, Data Migration and Long-Term Archiving for Ready Retrieval,”BioPharm 13 (6), 58-64 (2000).（日本語版は，W. Winter, L. Huber，近藤　直人，21 CFR Part 11 試験室における電子署名と電子記録；第四部　データ変換および長期保管，横河アナリティカルシステムズ，2001年6月，資料番号TI 16C0A3-007）

(5) W. Winter and L. Huber,“Implementing 21 CFR Part 11 in Analytical Laboratories: Part 5, The Importance of Instrument Control and Data Acquisition,”BioPharm 13 (9), 52-56 (2000).（日本語版は，W. Winter, L. Huber，近藤　直人，21 CFR Part 11 試験室における電子署名と電子記録；第五部　装置制御とデータ取り込みの重要性，横河アナリティカルシステムズ，2001年9月，資料番号TI 16C0A3-008）

(6) Committee on Information Systems Trustworthiness, Trust in Cyberspace［情報システムの信頼性に関する委員会、サイバースペースを信用する］, F.B. Schneider, Ed. (National Academy Press, Washington, DC), 22 December 1998. Available at http://cryptome.org/tic.htm.

(7) A. Miller, Risks in Biometric-Based Authentication Schemes［バイオメトリックベースの認証スキームにおけるリスク］, Information Security Reading Room (SANS Institute, Bethesda, MD), 2000. Available at www.sans.org/infosecFAQ/biometric.htm.

(8) Office of Regulatory Compliance, Code of Federal Regulations, Title 21, Food and Drugs: Electronic Records; Electronic Signatures［規制適合性局、連邦規制のコード、タイトル21、食品と医薬品：電子記録；電子署名］, Title 21, Part 11 (U.S. Government Printing Office, Washington, DC), issued March 2000. Also Federal Register 62 (54), 13429−13466. Available at www.fda.gov/ora/compliance_ref/part11.

(9) J.D. Woodward,“Believing in Biometrics［バイオメトリクスを信じること］,”Information Security (February 1998). Available at www.infosecuritymag.com/biometrics.htm.

(10) Immigration and Naturalization Service, How Do I Apply for INSPASS? ［INSPASSの申込方法］ (U.S. Department of Justice, Washington, DC), last modified 11 August 1999. Available at www.ins.usdoj.gov/graphics/howdoi/inspass.htm.

(11) Positive Identification in Health Care Systems［健康管理システムにおける実際的な認証］, NEC Technologies, Inc. (Itasca, IL, 1998).

(12) R.D. McDowall,“Biometrics: The Password You'll Never Forget［バイオメトリクス：絶対に忘れてはいけないパスワード］,”LCGC Eur. 13 (10), 734-742 (2000).

(13) B. Schneier,“Biometrics: Uses and Abuses,”Inside Risks 100［「バイオメトリクス：使用と乱用」、100のリスクの内側］, Communications of the ACM, 42 (8), Counterpane Internet Security, Inc. (San Jose, CA), August 1999. Available at www.counterpane.com/insiderisks1.html.

(14) Organisation for Economic Co-Operation and Development, Cryptography Policy: The Guidelines and the Issues［OECD、暗号化ポリシー：ガイドラインと発刊］, March 1997. Available at www.oecd.org/dsti/sti/it/secur/index.htm.

(15) R. Moskowitz,“Are Biometrics Too Good?”［バイオメトリクスはそんなに良いか？］Network

Computing, Issue 1002 (25 January 1999). Available at www.techweb.com/se/directlink.cgi?NWC19990125S0017.

(16) Security of Electronic Information Audit Guideline［電子情報監査ガイドラインのセキュリティ］, Issue 1.0 (Office of Information Technology, Sidney, Australia), 21 January 1998. Available at www.oit.nsw.gov.au.

© Agilent Technologies, Inc. 2002
Printed in Japan, September 09, 2002
5988-0947JAJP

本書の一部または全部を無断複製することは禁止されています。
記載内容は、お断りなく変更することがありますのでご了承ください。

http://www.agilent.co.jp/chem/yan
横河アナリティカル システムズ株式会社